CYBERSECURITY

SYSTRA

Resilient transport infrastructure
No trust without cybersecurity

PROTECT YOUR ESSENTIAL SERVICES

Transport systems are complex, highly interconnected and the impact of a cybersecurity attack is potentially major at operational, safety, reputational and financial levels.

For brownfield projects, it is up to the transport authorities and operators to identify existing assets, assess the risks (e.g. safety critical incident, loss of operations control, data leak...), then put in place organisational and technical measures to mitigate them. Main challenges are:

- Wide geographic distribution of assets along the railway line;
- Increasing mix of legacy systems (e.g. bespoke stand-alone systems) with new connected technologies (e.g. standardised COTS, open-source platforms, remotely accessible ICS and other IoT);
- Tough patch management and protection of outdated components due to systems warranty conditions;
- Eligibility to both cybersecurity and safety requirements.

For the construction of new lines, it is a matter of integrating cybersecurity issues into design and conception choices and setting up processes to adapt systems to the changing threat.

Cybersecurity becomes essential to deliver more connected and resilient transport services. Many transport infrastructures are considered as critical by national authorities, and submitted to security regulations such as NIS Directive in Europe or LPM in France.

SECURITY LEVEL TARGET

IEC 62443 standard "Security for Industrial Automation and Control Systems" defines four Security Levels.

SL1 ($)

Relevant protection against opportunistic threats

› *as a minimum*

SL2 ($$)

Relevant protection against hackers & cybercriminals

› *for better availability, detection, and resilience*

SL3 ($$$)

Relevant protection against hacktivist & terrorist organisations

› *for centralised security management*

SL4 ($$$$)

Relevant protection against governmental organisations

› *for advanced security*

Railway infrastructure managers and operators are quite vulnerable to cyber threats: governance and protection measures are partly implemented whereas detection and response measures are rarely implemented.

Majority of known cyberattacks on railway systems are opportunistic, but logging and detection means are lacking to investigate this further.

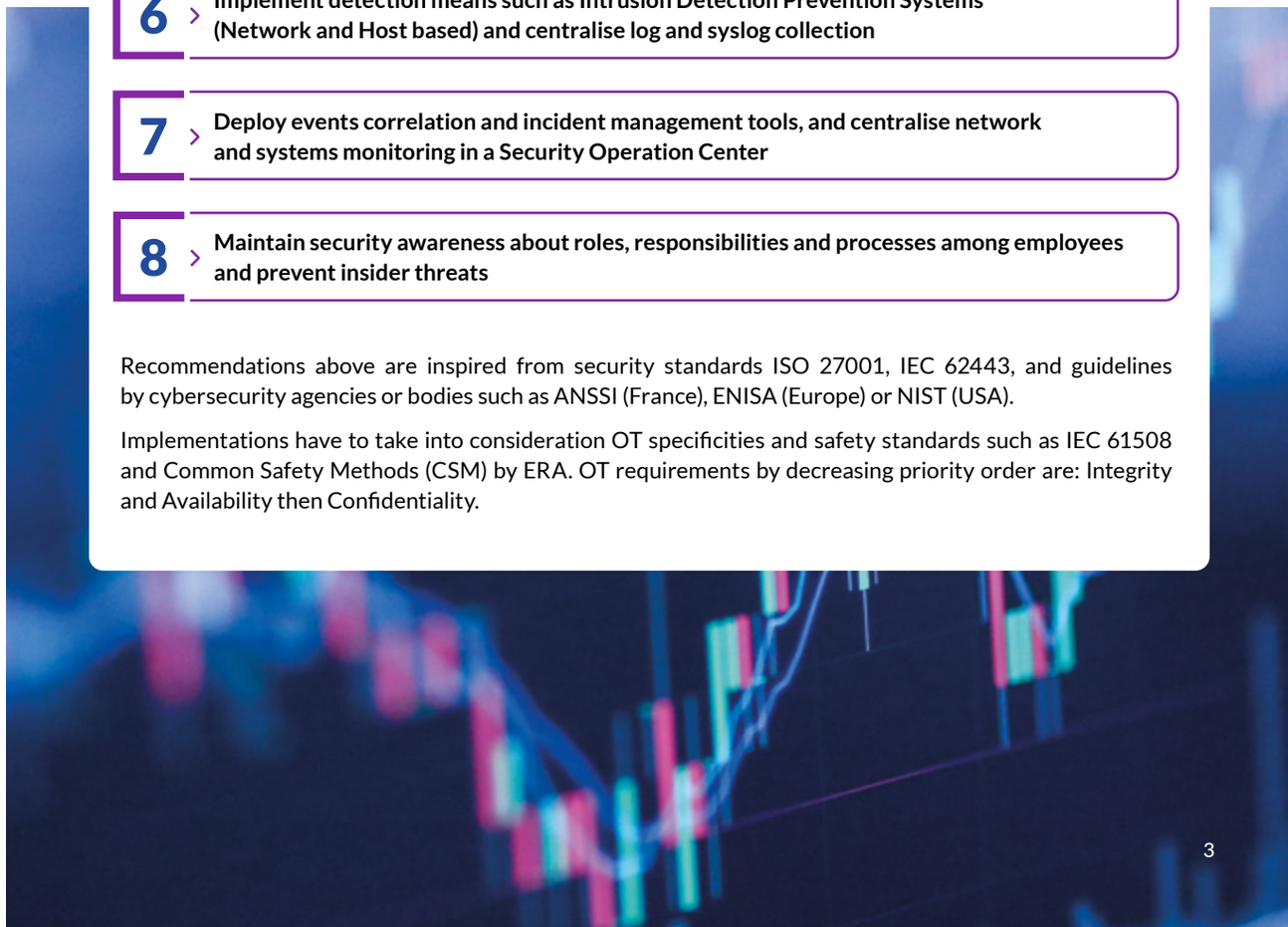
Finally railway infrastructure managers and operators remain vulnerable to Advanced Persistent Threats (APT) which would decide to specifically target Operational Technologies (OT).

RECOMMENDATIONS IN A NUTSHELL

1. **Map assets and identify critical targets according to impact assessment**
2. **Investigate threats, vulnerabilities and evaluate likelihood of threat scenarios**
3. **Harden and patch systems configuration, enforce zone segmentation and perimeter protection with firewalls, gateways or data diodes**
4. **Apply resilience mechanisms from IT (such as backup and recovery strategies) to OT and legacy systems, or define organisational countermeasures**
5. **Strenghten and unify physical and logical access control following a role based approach (RBAC) and the least priviledge principle**
6. **Implement detection means such as Intrusion Detection Prevention Systems (Network and Host based) and centralise log and syslog collection**
7. **Deploy events correlation and incident management tools, and centralise network and systems monitoring in a Security Operation Center**
8. **Maintain security awareness about roles, responsibilities and processes among employees and prevent insider threats**

Recommendations above are inspired from security standards ISO 27001, IEC 62443, and guidelines by cybersecurity agencies or bodies such as ANSSI (France), ENISA (Europe) or NIST (USA).

Implementations have to take into consideration OT specificities and safety standards such as IEC 61508 and Common Safety Methods (CSM) by ERA. OT requirements by decreasing priority order are: Integrity and Availability then Confidentiality.



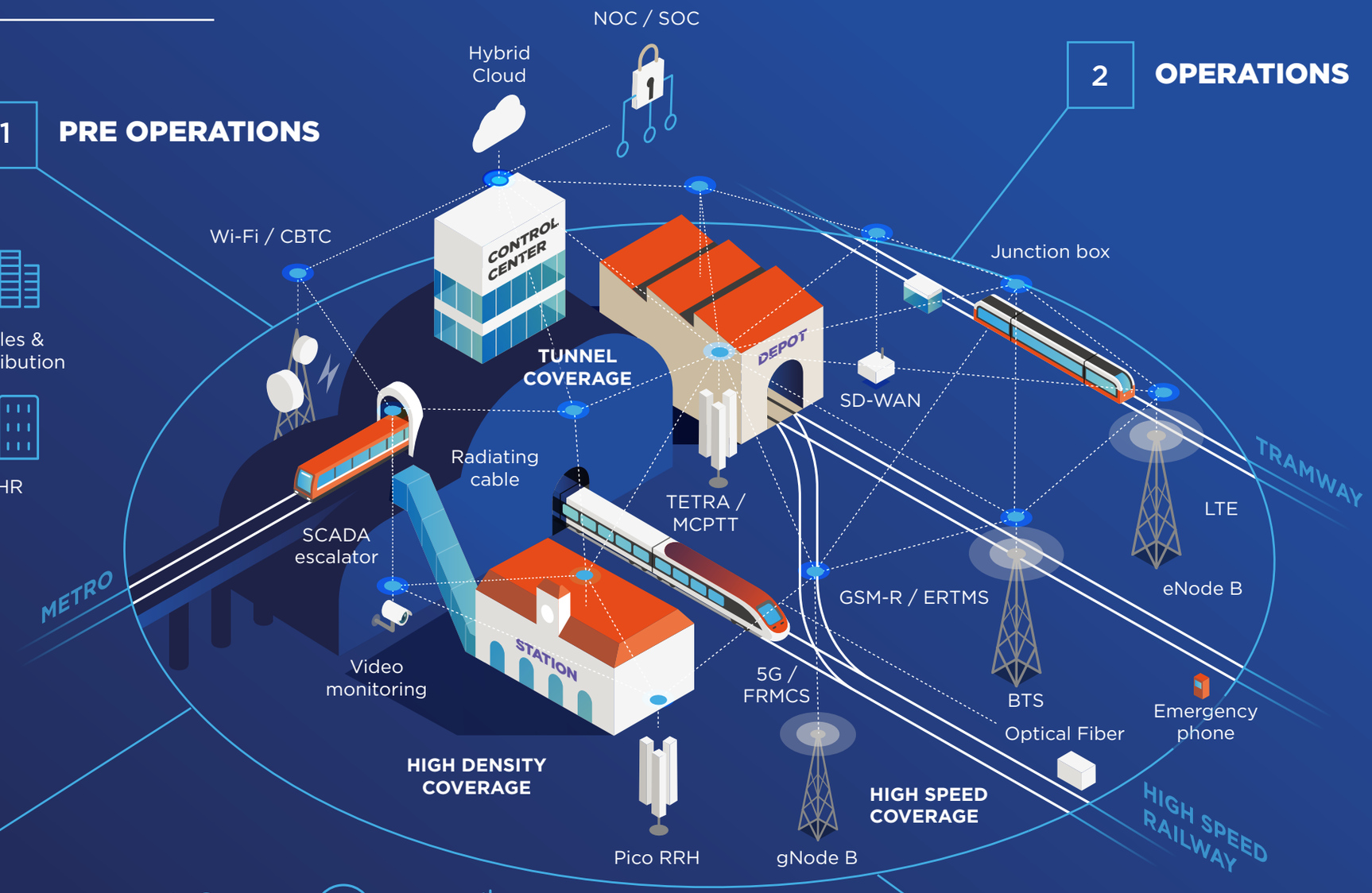
ENSURE BUSINESS CONTINUITY AND SAFETY

1 PRE OPERATIONS

- Network allocation
- Procurement & Logistics
- Sales & Distribution
- Corporate & Finance
- HR

2 OPERATIONS

- Signalling
- Command Control
- Telecom
- Auxiliary



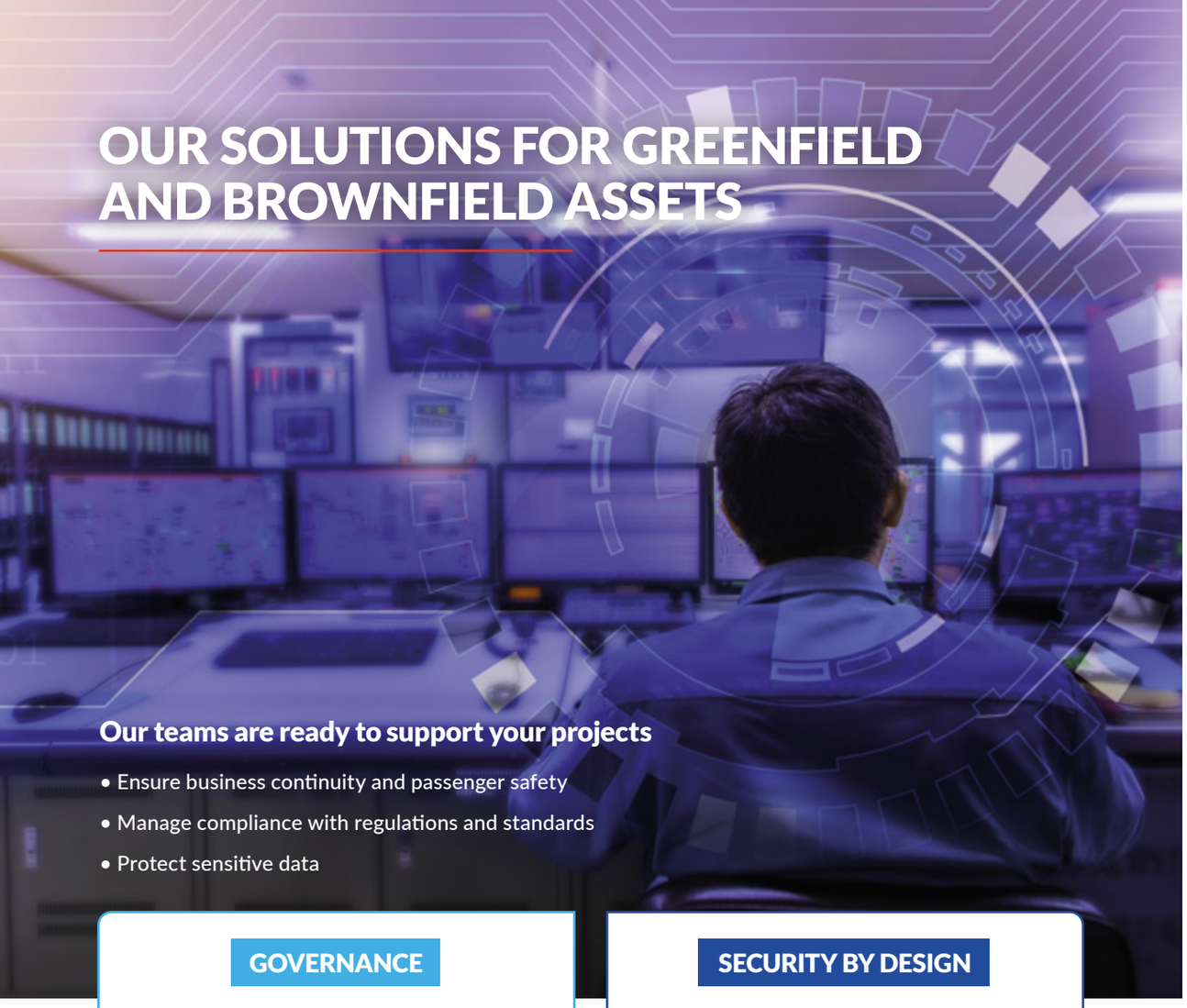
4 PASSENGER EXPERIENCE

- Escalator
- Lighting
- HVAC
- Entertainment
- Wi-Fi
- Public announcement
- Passenger information display
- Ticketing, Registration & Fare collection
- Call centre

3 SAFETY, SECURITY & MAINTENANCE

- Fire detection
- Video protection
- Diagnosis
- Access control
- Emergency telephony & Alerts
- Network monitoring & Cybersecurity
- Asset management

OUR SOLUTIONS FOR GREENFIELD AND BROWNFIELD ASSETS



Our teams are ready to support your projects

- Ensure business continuity and passenger safety
- Manage compliance with regulations and standards
- Protect sensitive data

GOVERNANCE

Define your security strategy and increase resilience of your organisation

AWARENESS

RISK ANALYSIS

SECURITY POLICY

SECURITY BY DESIGN

Manage security throughout your project lifecycle

REQUIREMENTS

DESIGN REVIEW

IMPLEMENTATION REVIEW

VULNERABILITY ASSESSMENT

Map your assets, vulnerabilities and enforce security

INVENTORY

INTERNAL AUDIT

COMPLIANCE

INTEGRATION OF SOLUTIONS

Select relevant solutions and manage a seamless deployment

STUDIES

DESIGN

IMPLEMENTATION

OUR ECOSYSTEM

ZOOM: AGILE RISK MANAGEMENT

Decision making requires having a clear overview on priorities being supported by an incremental risk management process.

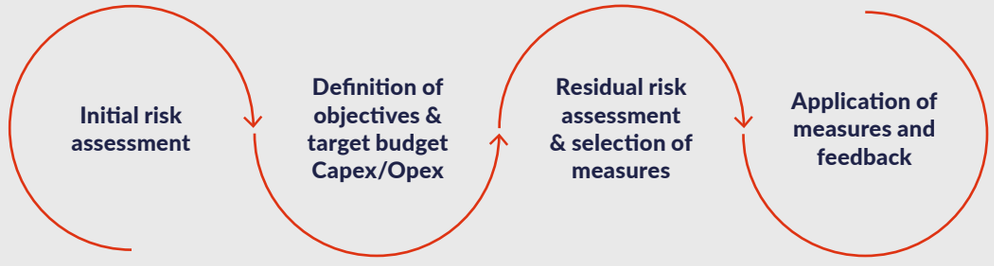
The EBIOS Risk Management methodology by ANSSI (compliant with ISO 27005) promotes a dynamic and threat centric approach, paying attention to the analysis of threat scenarios at strategic and operational levels.

Risk scoring has to take into account impacts (operational, safety, financial) and threat likelihood.

Likelihood of threat scenarios can be computed according to the analysis of past cyberattacks and upcoming threats.

New security exploits are made public every month revealing new weaknesses in transport systems and infrastructures. They can be packaged in order to simplify or industrialise their use.

As technological changes continuously arise (e.g. 5G, FRMCS, Cloud, IoT, etc.) with significant impacts on the vulnerability exposure, security measures shall be adapted as quickly as possible.



OUR MAIN REFERENCES

STAKEHOLDERS MAPPING AND MINIMUM-SECURITY MEASURES IN THE RAIL SECTOR

CONTRACTOR: ENISA (European cybersecurity agency), Europe, 2020

Under the framework contract "Supporting cybersecurity for transport sector activities - Lot 2 - cybersecurity for the railway sector", SYSTRA carried out a study, a survey and interviews to assist ENISA to evaluate the NIS Directive implementation in the rail transport sector. SYSTRA supported ENISA in the following tasks:

- Analysis of standards and existing regulations (e.g. ISO 27001/2, IEC 62443, draft TS 50701, DIN VDE 831-104, NIST CSF, NIST 800-82, APTA, ANSSI ICS guidelines, NIS Directive, LPM)
- Review of predefined security measures applicable to railway systems
- A survey targeting railway infrastructure managers and operators
- Drafting report, summary report and press-release

SIGNALLING ENCRYPTION FOR A RAILWAY TRACK IN NORTH-AMERICA

CLIENT: Railroad, USA, 2016-today

SYSTRA designs and implements a One Time Password framework for the PTC radio communication.
SYSTRA performs the following tasks:

- Analysis of client needs and railway operators' constraints
- Assessment of threats, vulnerabilities and risk analysis
- Specifications writing, then software development follow up
- Source code analysis with a vulnerability analyser
- Keys management program and PKI implementation for edge and ground devices
- OTP implementation for traffic light crossing
- Procurement of onboard assets and implementation in the new trainset product line
- Lab and Field Tests and demonstration as part of the certification process
- Personnel training, and advisory services to update operational procedures

AUTOMATED TRAIN CONTROL SYSTEM IN AUSTRALIA

CLIENT: Transport Authority, Australia, 2014-2016

SYSTRA checked the design of the telecommunication infrastructure with signalling system requirements (GSM-R, signalisation). It consisted in analysing the actual architecture and identify improvements in order to enhance the performance and security. SYSTRA performed the following tasks:

- Analysis of the actual infrastructure and network classification regarding EN 50159 standard
- Risk analysis
- Cybersecurity guidelines for the telecommunication network

CYBERSECURITY CONSULTANCY SERVICES FOR A PUBLIC METRO OPERATOR

CLIENT: Public Metro Operator, Asia, ongoing

SYSTRA acts as project management consultant on the metro systems (4 lines, 37 stations).
SYSTRA performs the following tasks:

- Analysis of local regulations
- Risks analysis (according to ISO 27005)
- Design review and analysis of system interfaces
- Security policy (according to ISO 27001/2)
- Implementation of the security policy and support to governance
- Definition of compliance and test procedures
- Definition of pentests strategy and scenarios, then follow-up
- Studies about the implementation of a Security Operations Center

CYBERSECURITY ADVISORY SERVICES FOR A TRAMWAY TURNKEY CONTRACTOR

CLIENT: Tramway Turnkey Contractor, Asia, completed

SYSTRA provides advisory services and performs the following tasks:

- Design review
- Asset inventory and analysis of systems interfaces
- Systems architecture audit
- Analysis of local regulations
- Security policy and local rules
- Initial and detailed risk analysis (according to ISO 27005)
- Support to governance
- Implementation of technical measures in cooperation with authorities

SYSTRA'S ADDED VALUE:

- **Knowledge of transport systems including telecom, command-control, signalling, auxiliary systems and passenger services**
- **Expertise in cybersecurity for OT (Operational Technologies)**
- **Ability to address both security and safety**
- **Involvement in security working groups and standardization bodies such as CENELEC WG26 and ER-ISAC**

www.systra.com
systems@systra.com

SYSTRA

SYSTRA Australia
Level 15 - Chifley Tower
2 Chifley Square
Sydney NSW 2000
AUSTRALIA

SYSTRA France
72-76, rue Henry Farman
75015 Paris - FRANCE
Tél. : +33 (0)1 40 16 61 00

SYSTRA Singapore
333 North Bridge Road
#05-01 KH KEA
Singapore 188721
SINGAPORE

SYSTRA UAE
Al Masraf Tower
Dubai
UNITED ARAB EMIRATES

SYSTRA LTD - UK
3rd Floor, 5 Old Bailey,
London, England, EC4M 7BA
UNITED KINGDOM

SYSTRA USA
New York Headquarters
520 Eighth Avenue, Suite 2100
New York, NY 10018 - USA

CONFIDENCE MOVES THE WORLD